Navigating the Policy Compliance Roadmap for Small Satellites

Barbara Braun, Sam Myers Sims
The Aerospace Corporation
PO Box 80360 Albuquerque, NM 87198; 505-846-8413
barbara.braun@aero.org

Kenneth Reese, David Butzin
USAF SMC/ADSS
3548 Aberdeen Ave SE Kirtland AFB NM 87117-5776; 505-853-3095
kenneth.reese@us.af.mil

David Voss
USAF AFRL/RVEP
3550 Aberdeen Ave. SE
Kirtland AFB NM 87117-5776

ABSTRACT

The Department of Defense (DoD) Space Test Program (STP) is charged with providing access to space for experiments on the DoD Space Experiments Review Board (SERB) list. Additionally, STP is the “front door” for all non-DoD Auxiliary Payloads seeking launch opportunities on DoD missions. In this capacity STP manages the launch integration of a wide variety of missions, including not only DoD satellites, but also satellites built, owned, and operated by the National Aeronautics and Space Administration (NASA), civilian universities, commercial entities, and foreign governments. Often a single launch mission has multiple satellites from multiple organizations, and may also contain payloads from one organization hosted on satellites owned by another.

As the launch integration manager for all of these satellites and hosted payloads, STP is faced with the challenging task of understanding the space policy requirements for a diverse set of agencies, and guiding its mission partners through the approval process. As small satellites and rideshares lower the barriers to space access, we see increasing numbers of mission managers who are unsure of what policies are applicable to their missions, and the steps they must take to demonstrate compliance. In addition, many of STP’s missions fall into policy “grey areas,” where policy and approval processes are not yet well-defined. In particular, the policy implications of imaging capability, frequency coordination, cybersecurity, proximity operations, and space debris mitigation are complex, poorly understood, and constantly evolving. Furthermore, the policy compliance and approval process is always one of the biggest “long-lead items” on any satellite’s schedule, and is particularly challenging for small satellites with short build cycles and limited staff.

This paper explores United States space policies and how they apply to satellite missions that may not fit the typical satellite mission mold. The paper presents a “roadmap” for policy compliance for satellites from diverse agencies, and identifies areas where further work is underway to address the challenges posed by the evolution of the space industry. The paper and presentation lay out a coherent way forward for all small satellites navigating the approval quagmire, and for mission managers of multi-payload rideshares who wish to smooth the path to launch approval.

INTRODUCTION

In the early days of satellite development and launch, only governments or government contractors built satellites and rockets, and generally each launch carried only a single satellite to orbit. Today, the space enterprise encompasses many players, including not only governments and large corporations, but also small businesses, universities, and even high schools and affinity organizations. The proliferation of small satellites has led not only to large numbers of new entrants into the space business, but also to an increasing number of rideshares, and the paradigm of a single launch carrying a single mission to space is no longer the norm.

The Department of Defense (DoD) Space Test Program (STP) has faced this reality for many years. Charged with providing access to space for experiments on the DoD Space Experiments Review Board (SERB) list,
STP is also the “front door” for all non-DoD Auxiliary Payloads seeking launch opportunities on DoD missions. In this role, STP frequently manages rideshares of diverse satellites from multiple agencies, including not only DoD satellites, but also satellites built, owned, and operated by the National Aeronautics and Space Administration (NASA), civilian universities, commercial entities, and foreign governments.¹

As the launch integration manager for such missions, STP is faced with the challenging task of understanding the space policy requirements for a diverse set of agencies, and guiding its mission partners through the approval process. STP has worked with the staff of the office of the Principal DoD Space Advisor Staff, (PDSAS, formerly SAF/SP), SAF/AQR (Air Force Acquisitions, Space Programs), the Air Force Research Laboratory (AFRL), as well as NASA and other civilian agencies, to clarify policy applicability, and identify where policy “boundaries” exist. In this paper, we explore United States (US) space policies and how they apply to satellite missions that may not fit the typical satellite mission mold, on launch missions that may not have a single responsible agency. Where applicable, we have outlined the processes and approvals involved in getting to space. In addition, we have identified where further work is required to fill in policy gaps and “gray areas” in the overall policy picture.

Like the space industry itself, policy is constantly evolving. While we have tried to capture the current “policy roadmap” as accurately as possible, we welcome corrections and updates from the community as the picture comes into better focus.

**POLICY OVERVIEW**

*International Treaties and US National Policy*

The Outer Space Treaty of 1967² forms the basis of international space law, and stipulates that states “shall be responsible for national space activities whether carried out by governmental or non-governmental agencies.” It places the responsibility for operations in space on the government of the nations that fly in space, and requires “authorization and continuing supervision” by that government. In the Outer Space Treaty, a nation “on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such object....” This implies that the US government has responsibility over US-owned objects in space, regardless of whether that object is launched by the US or by a foreign launch provider. Similarly, foreign satellites remain the property of foreign entities, even if launched from a US rocket. While the Outer Space Treaty places joint liability for damage on the country “from whose territory or facility a space object is launched” as well as the country that procured the launch, this liability is only absolute for damages on Earth and to aircraft in flight. For damages in space, the launching country shall be liable “only if damage is due to its fault or the fault of persons for whom it is responsible” – in other words, only if the damage is due to the launching country’s negligence or malicious intent.

Within the US, National Space Policy (NSP)³ also directs safe and responsible operations in space. Specific sections discuss protection of the space environment (including debris mitigation) and protection of the electromagnetic spectrum. The NSP also references “the critical interdependence of space and information systems,” which will flow into lower-level guidance on cryptographic protection of space systems. Similarly, the National Space Transportation Policy⁴ outlines the authorities for military, civil, and commercial launch oversight. Military oversight is provided by the DoD; civil oversight is provided by NASA. Commercial space transportation oversight is under the Secretary of Transportation; thus, commercial launches are licensed by the Federal Aviation Administration (FAA).

**The Responsibilities of the Launch Provider vs. Satellite Owner**

The National Space Transportation Policy, true to its name, discusses mainly access to space in the form of launches, rather than operations in space once satellites have separated from the launch vehicle. Similarly, most lower-level policy demarcates the responsibilities of the launch provider and the responsibility of the spacecraft owner / operator at the point where the spacecraft separates from the launch vehicle or its upper stage.

In other words, the launching agency is not (and should not be) the policy gatekeeper for the satellites it launches; it cannot be, because once launched, these satellites are no longer necessarily under the authority or direction of the launching agency. Without the ability or authority to enforce policy throughout the satellite’s orbital lifetime, the launching agency cannot ensure compliance. Instead, compliance must be enforced through the parent agency of the satellite owner / operator. Thus, a NASA satellite launched on a DoD rocket must demonstrate compliance with NASA policy, not DoD policy. Similarly a DoD satellite on a commercial launch must still demonstrate compliance with DoD policy, not commercial policy. Figure 1 illustrates the general responsibilities of mission partners on a launch mission, and Figure 2 illustrates in more detail how these policy responsibilities break down for a sample multi-payload mission.
In developing multi-payload missions, STP has found clarifying this demarcation increasingly important to establishing the proper policy compliance responsibilities for its satellite provider partners. Note that this approach does not preclude the launching agency from imposing its own more stringent requirements, or even its own parent agency’s policies, on the satellites it launches. The launching agency may still “refuse service” to a satellite that does not meet certain requirements, even if those stipulations are not required by policy.

**What Constitutes Ownership?**

Determining the parent agency of the satellite is, therefore, critical to understanding the applicability of US space policy. The flowchart shown in Figure 3, developed in partnership with AFRL, illustrates STP’s method for determining satellite ownership. The key consideration is, “who will have control authority over the satellite (or payload) once it launches?” If the DoD makes the decisions for all spacecraft activities after launch (commonly referred to as Satellite Control Authority, or SCA), then it is a DoD satellite, regardless of whether or not it is built, or operated, by a private company. Similar rules apply to NASA satellites, with the additional stipulation that NASA contracts and NASA grant recipients are also considered NASA satellites.

STP frequently arranges for the launch of private university satellites sponsored to the DoD SERB by military sponsoring agencies. Some of these satellites are part of Air Force Office of Scientific Research (AFOSR) / AFRL University Nanosatellite Program (UNP) a Science Technology Engineering and Math program. Although sponsored by UNP, ownership of the vehicle and SCA remain with the universities. The universities are private entities, and therefore such payloads currently follow a commercial path to comply with policy regulations, not a DoD path. Discussion continues on this point, however, and this remains an area where further policy clarity is needed.

Also needed are discussions about “special cases,” such as civil government satellites that are non-DoD, non-NASA satellites. Later sections will also discuss the

---

**Figure 1: Policy Compliance and Safety Responsibilities for Launch Missions**

**Figure 2: Rideshare Policy Compliance for Individual Payloads**
special case of DoD satellites that are not National Security Space (NSS) satellites, as these highlight other policy gray areas that require further clarification.

Once the owning organization is identified, the appropriate policies can also be identified. The DoD, NASA, the FAA, and the Federal Communications Commission (FCC) all have broad policy directives that flow down from the NSP; these will be discussed in more detail in the applicable sections of this paper. In particular, we will discuss orbital debris mitigation policy, frequency allocation and spectrum usage, information assurance, imaging, and rendezvous and proximity operations.
ORBITAL DEBRIS POLICY

National Policy

As described above, the US NSP calls for protection of the space environment from orbital debris. Specifically, one of the Intersector Guidelines directs compliance with US Orbital Debris Mitigation Standard Practices (ODMSP), and requires “the head of the sponsoring department or agency” for space missions to approve exceptions. The ODMSP itself has four sections, governing debris generation, accidental explosion, minimizing the risk of collision with other objects, and disposal of space objects at the end of mission life. Tether systems have special considerations in the ODMSP.

The ODMSP is the source of most of the debris requirements familiar to experienced satellite developers: the requirement for disposal within 25 years of the end of the mission, the requirement that re-entering space objects not cause casualties on the earth, and the requirement that limits the potential for in-space collision, debris generation, and accidental explosion. Because these guidelines are national, they apply to all US missions, but other than the 25-year disposal number and the 1 in 10,000 “expectation of casualty” number, the ODMSP does not contain specific numeric thresholds.

NASA Policy

NASA documents orbital debris mitigation requirements in NASA Procedural Requirements for Limiting Orbital Debris, and NASA Process for Limiting Orbital Debris. In this last document we find specific numeric limits to the probability of in-space collision (1 in 1000 over the lifetime of the mission), and accidental explosion (also 1 in 1000). The document lists other detailed requirements for compliance with the ODMSP. It also requires documentation of compliance in an Orbital Debris Assessment Report (ODAR), and an End of Mission Plan (EOMP). The ODAR and the EOMP are approved through NASA channels, and exceptions flow up through the NASA Office of Safety and Mission Assurance. It is worth noting that the National Oceanic and Atmospheric Administration (NOAA) satellites also follow NASA debris mitigation requirements.

DoD Policy

Department of Defense Directive (DoDD) 3100.10, Space Policy, states that the “DoD will promote the responsible, peaceful, and safe use of space, including following the U.S. Government Orbital Debris Mitigation Standard Practices.” In addition, Enclosure 2 of DoDD 3100.10 states that “the Secretaries of the Military Departments shall formulate and implement

Military Department-level space-related policies and programs that support … this Directive.” Department of Defense Instruction (DoDI) 3100.12, Space Support, requires that DoD missions comply with debris mitigation practices that echo the ODMSP. The Air Force has implemented DoDD 3100.10 and DoDI 3100.12 in Air Force Instructions 91-202, The Air Force Mishap Prevention Program, and 91-217, Safety and Mishap Prevention Program. The other DoD services have implemented the requirements in DoDD 3100.10 in different ways; the National Reconnaissance Office has an Office of Debris Mitigation, while the Army and the Navy have relatively informal coordination processes.

FCC Policy

Private satellites, defined in this case as any satellite not owned or operated by NASA, NOAA, or the DoD, do not fall under any of the NASA and DoD policies, but must still comply with national orbital debris mitigation guidelines. This compliance is enforced by the only agency that currently has the authority to regulate privately-owned US satellites in space: the Federal Communications Commission (FCC), through its licensing of uplink and downlink frequencies. Title 47 of the Code of Federal Regulations (CFR) requires applicants for frequency licenses to provide information on their orbits and their plans for orbital debris mitigation. FCC regulations also require the use of disposal options and the safining of pressure vessels at the end of life. An examination of online documents shows that many private satellites, when applying to the FCC, use NASA’s ODAR format to document their orbital debris mitigation compliance.

FAA Policy

The Federal Aviation Administration (FAA) licenses launch and reentry operations for non-government launches from US soil, or conducted by US companies or citizens. Contrary to popular belief, it does not oversee or regulate satellites in space. FAA regulations levy safety requirements on launch vehicles, including limiting the potential for debris generation and accidental explosions, and for reentry vehicles, limiting the potential for human casualty on the ground. The FAA, however, does not regulate the disposal of orbiting upper stages.
Policy Compliance Process

Once the owning / operating agency for a satellite is known (see Figure 3), that agency must demonstrate compliance with its parent agency’s orbital debris mitigation policy. For NASA, this involves the preparation and submittal of an SDAR and EOMP in accordance with the NASA Process for Limiting Orbital Debris. The process is similar for Air Force missions, which complete an ODAR/EOLP in accordance with AFI 91-217. Missions without defined processes or formats for debris compliance should consider using the NASA ODAR as the template for demonstrating compliance with higher policy, as seems to be the practice for private satellites when requesting licenses from the FCC. Launch vehicles should follow the FAA’s process through the “end of launch,” defined by the FAA as the last exercise of control over the launch vehicle. It is important to note that exceptions to ODMSP guidelines require approval at very high levels: the head of the sponsoring department or agency. Such waivers are increasingly difficult and time-consuming to get, suggesting that satellite missions should conduct the required analyses early in order to allow time for design changes or waiver approvals, as needed.

Ambiguity, Open Questions and Recommendations

The ODMSP guidelines represent one of the more well-known and universally accepted aspects of space policy, but policy gaps still exist. One of the biggest open questions is whether the FCC, whose mission typically has little to do with space, should be the agency to enforce orbital debris mitigation policy on the burgeoning commercial and private satellite business. Similarly, the lack of specific requirements for orbiting upper stages for non-DoD or NASA launches is a gap that policymakers must ultimately address. Also, it is important to note that although the orbital debris compliance requirement is 25 years after mission completion, all satellite owners should strive to dispose of the vehicle once the mission is concluded, as good stewards of space. Finally, many organizations lack specific policy guidance outlining the document format and approval authorities for orbital debris compliance. This can lead to confusion and ad-hoc approaches to compliance, in an area where clarity is badly needed.

SPECTRUM USAGE

Summary of Applicable Policy

Public law and regulations, rather than policy, provide all guidance for the assignment and usage of spectrum for satellites. The National Telecommunications and Information Administration (NTIA) regulates frequency usage for federal agencies such as NASA and the DoD. The NTIA documents their rules and procedures in the manual Radio Regulations, codified in Title 47 of the CFR.

The FCC licenses frequency use for non-federal agencies, including private and commercial satellites. The FCC documents their rules and regulations in Title 47 of the CFR. Part 25 contains information about commercial and remote sensing satellite communications. Part 5 covers experimental missions, and Part 97 covers amateur communications.

Additionally, the International Telecommunication Union (ITU) is the United Nations (UN) Specialized Agency responsible for telecommunications. The ITU does not have any authority to enforce policy, but the participating UN countries honor its treaty status. The ITU has its own rules and regulations codified in Radio Regulations.

Policy Compliance Process

The NTIA is located within the Department of Commerce (DoC) and is the agency responsible for managing the federal use of spectrum. Instructions for filing are laid out in the Manual of Regulations and Procedures for Federal Radio Frequency Management. The NTIA grants the authority to use a frequency, not a license. The Frequency Assignment Subcommittee (FAS), within the NTIA, coordinates and assigns radio frequencies. NASA programs work their submission through the individual center spectrum management office and then the NASA spectrum management office. The NASA spectrum management office will then submit paperwork to the NTIA. DoD-owned missions submit through service-level spectrum management offices, who then submit to the NTIA. There are four filing stages for federal programs: 1 – Conceptual, 2 – Experimental, 3 – Developmental and 4 – Operational; each is explained in detail in section 10.4.1 of the NTIA manual. Most small satellites performing science and technology (S&T) or research and development (R&D) missions will obtain a Stage 2 Experimental license. As the name indicates, operational satellites will obtain a Stage 4 Operational license. Unlike the FCC there is no requirement to conduct debris or lifetime analysis when applying to the NTIA for frequency usage.

The FCC is an independent US government agency (overseen by Congress) that regulates interstate and international communications by radio, television, wire, satellite, and cable in the US. Part 25 of CFR 47 outlines the application and filing process. Most small satellites will submit for either an amateur or an experimental frequency. The main difference is that amateur frequencies are for communications only, and the operator cannot have a financial interest on behalf of
Missions filing with the FCC must demonstrate compliance with the ODMSP guidelines, as described in the orbital debris section of this paper. Missions must show that they are not going to be a source of debris, that they will not cause debris, that they will deorbit within 25 years of end of life, and that they will not have an expectation of casualty other than zero when re-entering. If missions cannot demonstrate this satisfactorily to the FCC, they may be required to carry insurance or risk not be approved to broadcast.

When frequency usage is approved, the FCC and NTIA submit their frequency assignments to an FCC Liaison who then submits the US assignments to the ITU who maintains the international register. Getting a license or approval to use a frequency through either agency takes months to years, so missions should start working on the application and submittal as soon as possible.

**Ambiguity, Open Questions and Recommendations**

There is strict protection of the amateur frequencies from use by experimental or federal programs. This has led to some confusion in the community as to the ability to use amateur bands, particularly since until recently, experimental or federally-connected programs regularly used amateur bands. Programs who have previously used amateur bands are now having to figure out if they have to go through the FCC for an experimental frequency, or through the NTIA. For example, satellites being built and sponsored by the US Naval Academy have in the past used amateur frequencies, and operate an amateur ground station at the Academy. As a federal agency, however, it now appears they should file through the NTIA, and will no longer be allowed to file through the FCC to use amateur frequencies. As of the writing of this paper the matter has not been resolved, and the resolution has been hampered, in part, by the lack of clear communication between the FCC and the NTIA.

Additionally, there is often confusion for programs that fall into “gray areas.” For example, a university-owned and operated satellite that receives funding from the DoD and launches on a DoD launch vehicle remains a private satellite, but is sometimes directed to the NTIA for frequency approval. Occasionally, missions get different answers from the FCC and the NTIA. The future will probably bring more of these “gray area” missions, and it would be helpful to have a single office for frequency submittals. That office could then route the approvals to either the NTIA or the FCC, as appropriate to each mission.

**CYBERSECURITY/INFORMATION ASSURANCE**

**Summary of Applicable Policy**

Cybersecurity policy for small spacecraft is defined in a complex and confusing menagerie of policy documents published by the DoD, the Committee on National Security Systems (CNSS), the National Institute of Standards and Technology (NIST), and other organizations. For all spacecraft used by the DoD, a key document is DoDI 8581.01, *Information Assurance (IA) Policy for Space Systems Used by the Department of Defense.* This instruction implements CNSS Policy No. 12, *National Information Assurance Policy for Space Systems Used to Support National Security Missions.*

To determine if an information system is considered NSS, there is NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System.*

There are two DoD Instructions governing cybersecurity compliance for all DoD information systems (not just space systems). They are DoDI 8500.01, *Cybersecurity,* and the Risk Management Framework (RMF) for DoD Information Technology (IT), 2014. These two instructions align the DoD with the rest of the federal government by adopting common CNSS and NIST controls, particularly NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations.* This promotes interoperability, information sharing, and reciprocity, enabling organizations to accept approvals by other organizations for interconnection or reuse of IT without retesting. The RMF replaces the old DoD Information Assurance Certification and Accreditation Process (DIACAP), and a transition from DIACAP to RMF is underway.

**Policy Compliance Process**

There are two primary areas of compliance associated with spacecraft cybersecurity policy (although this is not exhaustive). The first concerns protection of the spacecraft uplink and downlink (i.e. the requirement for...
The second concerns certification and accreditation (C&A) requirements of the spacecraft as an information system (i.e. the requirement to receive an Authority to Operate, or ATO). These will be covered in turn.

**Encryption**

For DoD-owned or controlled spacecraft, DoDI 8581.01 requires encryption of the uplink and downlink. This applies to all DoD satellites, including R&D spacecraft built by DoD laboratories or academic institutions. Selection and implementation of the cryptography used to meet requirements should be coordinated with National Security Agency (NSA) early in the design phase of every spacecraft program.

For non-DoD Federal spacecraft (i.e. NASA), encryption is not strictly required. However NIST SP 800-53 does apply, and the criticality and sensitivity of information transmitted may lead to selection of security controls that include encryption. Organizational policies may also apply, for example NASA Procedural Requirements 2810.1A, *Security of Information Technology*, defines information technology security requirements for NASA.

For commercial or private spacecraft, encryption is not typically required. However if the DoD is using a commercial/private, non-DoD Federal, or foreign space system, DoDI 8581.01 has requirements pertaining to encryption. Depending on the criticality and sensitivity of the DoD information being transmitted, uplink and/or downlink cryptography may be required ranging from NSA-approved to commercial best practices. In order to obtain a NOAA commercial remote sensing license, there are rigorous conditions to incorporate safeguards to ensure the integrity of system operations and security of its data. Early coordination with NSA is recommended.

**Certification & Accreditation (C&A)**

DoDI 8581.01 requires that all DoD owned systems undergo cybersecurity accreditation in accordance with RMF. A full discussion of the RMF process is beyond the scope of this paper. However two points are worth mentioning. Each DoD spacecraft program should determine who their cybersecurity Authorizing Official (AO) is early in the program. The AO staff should be an invaluable resource, and the AO will ultimately issue the ATO for the spacecraft.

Non-DoD Federal spacecraft must follow their own internal policies regarding accreditation. Recent experiences with NASA indicate that formal C&A accreditation of the spacecraft (like a DoD ATO) is typically not required. For the GPIM mission on STP-2, NASA was required to issue an ATO to the spacecraft because it will be operated on an accredited DoD ground system.

Commercial and private spacecraft have no requirements to undertake a formal cybersecurity accreditation. When the DoD is using non-DoD systems, DoDI 8581.01 requires that the AO for the DoD organization using the system perform a review of the space system’s ability to meet cybersecurity requirements and accept the risk for any non-compliances.

**Ambiguity, Open Questions and Recommendations**

The first ambiguity has to do with whether a spacecraft should be considered “DoD” and therefore subject to DoD cybersecurity policy. There have been differing interpretations received, with the most stringent classifying any spacecraft receiving DoD sponsorship or funding of any nature as DoD and subject to all DoD policy requirements. This interpretation would have far reaching implications and is not considered tenable. As described in the section on satellite ownership, satellites should be classified unambiguously based on who is the owner/operator of the spacecraft. Cybersecurity policy compliance should be based on the requirements of the owner/operator organization.

A second ambiguity has to do with whether a satellite system is considered NSS. NIST SP 800-59 has a checklist with six questions to determine if an information system is NSS. Based on this checklist, many DoD R&D spacecraft developed and operated by military laboratories and academic institutions are not NSS. As such, CNSSP No. 12 is not applicable. However DoDI 8581.01 (which implements CNSSP No. 12) does not provide any provisions for non-NSS DoD spacecraft, which drives costly compliance requirements on these programs out of proportion to overall program cost and risk. DoDI 8581.01 should be revised to either explicitly exclude non-NSS DoD spacecraft or to provide streamlined compliance procedures for this class of spacecraft.

DoDI 8581.01 provides procedures for implementing cybersecurity when DoD uses non-DoD spacecraft. “Use” is not well-defined and subject to interpretation. It would be beneficial to expand this section of the policy to include different cases of “use”, such as hosted payloads, commercial imagery, and DoD sponsorship. Additionally, as hosting DoD payloads on non-DoD spacecraft becomes more common, cybersecurity requirements and responsibilities need to be better defined in memoranda of agreement up front.

Finally, there is no policy requiring the protection of non-DoD spacecraft command and control capability...
(particularly uplink encryption) when the spacecraft possesses significant delta-V capabilities. This is a significant policy hole that will become more pronounced with the increasing capabilities of small satellites and CubeSats; policy should be established requiring uplink security on all spacecraft with significant delta-V capability. This could be incorporated into the established process for securing an FCC frequency license. Federal organizations entering into agreements with foreign spacecraft should establish this requirement, particularly when the U.S. is providing launch services for the foreign spacecraft.

IMAGING

Summary of Applicable Policy

Remote sensing from a space platform falls into two distinct regulatory categories in the US, Earth Imaging and non-Earth Imaging (NEI). There are also two types of satellites considered, with one subtype. The two primary types are commercial (civilian) satellites and satellites owned and operated by the government. This second type has a subset of DoD academic institutions which fall into their own unique policy bucket. This section will explore the various policies that apply to each type of satellite in each regulatory category and provide a basic understanding of how to navigate the policy compliance process.

Satellites owned and operated by commercial entities and civilian academic institutions are governed by the National Commercial and Space Programs Act. This law governs Earth imaging and assigns authority to NOAA for licensing of the same. For these commercial and civilian academic institutions, NOAA will ensure all imagers also comply with DoD and Intelligence Community (IC) requirements for NEI.

In researching this section, the team was unable to identify any NASA guidance or documentation with respect to imaging approval. All imaging devices aboard NASA satellites and missions are handled internal to the Administration. Government agencies currently have no requirement to obtain licensing for Earth imaging. NEI for operational DoD systems is managed by the Defense Remote Sensing Working Group (DRSWG). Experimental DoD satellites are governed by interim guidance issued by the PDSAS. This interim guidance, issued in 2015, requires DoD experimental satellites with remote sensing capability to submit test plans, data protection plans, and technical specifications of their system and payloads to the PDSAS, through the Secretary of the Air Force Space Programs (SAF/AQS) office. If PDSAS determines a concern exist with respect to an experimental DoD satellite the issue is automatically referred to the DRSWG.

Policy Compliance Process

The compliance process for commercial and civilian entities is outlined on the NOAA Commercial Remote Sensing Regulatory Affairs (CRSRA) website. NOAA recommends beginning the process with informal, non-binding meetings between the applicant and NOAA to help inform the process and prevent rework. When an organization is prepared to begin the application process, Code of Federal Regulations Title 15 Part 960 establishes the rules and procedures to be followed and NOAA provides support to ensure all the required documentation is provided. Part 960 consists of four subparts and two appendices which lay out the application process and filing instructions, the terms and conditions of a granted license, the appeals process, prohibitions associated with licensing, the enforcement procedures for licensees and non-licensees, and the requirements levied on NOAA through the DoC regarding the stakes of other government parties with respect to imaging licenses. All license determinations are required to be made within 120 days of receipt of a completed application unless written guidance is provided on issues that exist with the application. All licenses are valid for the operational lifetime of the system unless voided through action of the owner or operator.

Ambiguity, Open Questions and Recommendations

The DoD and Federal Government are in the process of providing clearer policy guidance for military academic institutions and satellites that are part of UNP. Until this definition is provided in final guidance those organizations should continue working through STP and UNP to obtain appropriate guidance.

RENNDEZVOUS AND PROXIMITY OPERATIONS

Summary of Applicable Policy

Current proximity operations policy is a patchwork set of policy and guidance across the space community. As the capability of small satellite systems increases, the desire for missions to perform proximity operations becomes more of a reality. Spacecraft designers must balance the need to perform mission objectives with safety of flight concerns. Although not necessarily proximity operation, safety of flight concerns extend to formation flying missions which intend to maintain a constant relative distance to each other. NASA currently has no policy guidance concerning proximity operations. There is a policy in the DoD for the review of proximity operations missions, but this policy may not be widely available. Neither the FCC nor the FAA has any policy compliance requirements for on-orbit proximity operations.
Policy Compliance Process

DoD missions intending to perform proximity operations missions must comply with DoD processes. Civil and commercial entities are currently not required to comply with any process unique to proximity operations objectives, although missions will naturally need to comply with all frequency and imaging requirements discussed above.

Ambiguity, Open Questions and Recommendations

With the growth in capability of small satellites there has been a surge in formation flying and rendezvous, proximity, and docking missions. Due to the extreme technical challenges of performing these missions and the inherent safety of flight concerns, clarification on processes for civil and commercial entities would be beneficial. The policy should distinguish between formation flying and proximity operations based off relative distance to space vehicles and define policy guidance for each class. Key to this guidance should be directives based off the amount of delta-V each space vehicle intends to carry. This should inform the cybersecurity posture of the vehicle and ground system. A related issue that needs to be captured (possibly in this policy) is cybersecurity requirements for vehicles with propulsion. Care should be taken to separate policy requirements for significant translational propulsion systems from those required for simple attitude control propulsive systems. It is recommended for both formation and proximity operations missions that mission designers comply with NIST SP 800-53 and implement commercial best practice encryption on the uplink and downlink.

POLICY “FLOWCHART” AND SAMPLE WALKTHROUGH

Figures 3-7 summarize all the policy pathways described in this paper, to the extent that the authors understand the existing policy framework. Starting in Figure 3, above, missions must first determine who “owns” the satellite, in order to determine what policy applies. Typically, the ultimate satellite owner / operator – whoever will have satellite control authority once the satellite is operational – is the agency whose policy the mission must follow. Once the mission ownership is understood, the remaining figures (Figures 3 through 7) describe the applicable policy.

As an example, if AFRL builds a satellite intending to conduct unclassified proximity operations, the Air Force is the owner / operator, and the DoD policy flowchart should be followed. DoD satellites are required to abide by information assurance requirements as documented in DoDI 8581.01; and even if the mission is unclassified, must use NSA-approved encryption. Such a satellite would apply to the NTIA for frequency assignment. If the satellite will perform proximity operations, DoD proximity operations regulations must be followed.

As another example, assume a private company builds a commercial satellite capable of imaging and conducting stationkeeping, and brings it to the DoD SERB for consideration. Even with SERB sponsorship, the satellite is still considered a commercial / private satellite, and will follow public policy for privately-owned satellites. It will apply for a frequency license through the FCC, and apply to NOAA for imaging approval. As part of its FCC filing, it will demonstrate its compliance with the ODMSP. However, there is no existing policy requiring such a satellite to encrypt its uplink or downlink, nor is it required to get approvals to conduct proximity operations. These are policy gaps that must be filled.

CONCLUSION

The policy picture for today’s rapidly-evolving space enterprise is complex and confusing, particularly to non-traditional entrants and missions that occupy policy “gray areas.” In this paper, we have attempted to clarify the applicability of existing policy, and outline a process for missions to follow to ensure compliance. We have also attempted to highlight areas where policy is absent or unclear. STP is in the process of applying this “roadmap” to its ongoing STP-2 mission, as well as future missions currently in work. It is, however, important to remember that the policy roadmap is always “under construction,” and that future changes are certainly expected. As the space enterprise evolves we hope that US policy will be agile enough to evolve with it, to ensure both access to space for all, and safety in space for all.

Figure 4: Key to Policy Roadmap Flowcharts

Braun 10 30th Annual AIAA/USU Conference on Small Satellites
DoD

Figure 5: Policy Roadmap Flowchart for DoD Satellites
Figure 6: Policy Roadmap Flowchart for NASA satellites
Figure 7: Policy Roadmap Flowchart for Private Satellites

Note the lack of consolidated public policy for many aspects of on-orbit operations, including prox ops and translational propulsion. Policy recommendations to SREB missions are based on STP interim guidance, but overarching policy is needed.
ACKNOWLEDGMENTS

The authors would like to acknowledge the help and support of the STP-2 mission team and in particular, Austin Potter of AFRL, who developed the first versions of the policy roadmap flowcharts.

REFERENCES

7. “Compendium of Space Debris Mitigation Standards Adopted by States and International Organizations”, March 25, 2014, Committee on the Peaceful Uses of Outer Space, Vienna, Austria
27. “United States Code Title 51: National Commercial and Space Programs”, December 18,